Action Item #	Action Item Description	RSIS Response	CDR Briefing Summary
PDR-T1-020904-100	Discuss safety engineering considerations. This would show that safety requirements are identified and that processes are in place to avoid injury or death.	Slide 86 discusses the safety engineering considerations that have been taken into account thus far. With the design still evolving, additional saftey considers will be reviewed at CDR.	Human Factors and Safety Engineering - Slide 39
PDR-T1-020904-14	Need to address FAA redundancy requirement (slide 85)	Concur - we are addressing the FAA redundancy requirement. Meetings are in progress with representatives from the AOS-250 group. Regular updates are provided to the COTR. Final presentation to be briefed at CDR.	FAA Redundancy Requirement - Drawings provided Slide 59, 64, 94. We conducted TIMs on 10 Feb 03, and 19 Feb 03.
PDR-T1-020904-18	Need to address Power Management requirement (slide 84)	Concur - Detailed power management design requirements will be provided to the ROC and FAA for review. Final presentation at CDR. The Action Item was added to the Risk List.	Power Management Discussion - Slides 61-65
PDR-T1-020904-21	For NWS Systems, will the legacy CSU be retained? One use of these CSU's were to provide a remote loopback capability to test the T1 circuit end-to-end.	We are evaluating the router's requirements and capabilities. As of 9/13/02, the plan is to keep the legacy CSU as reflected in the cabinet drawing. Detailed design briefed at CDR.	The Legacy CSU will be replaced with Cisco. NWS Systems - Drawings provided Slide 94
PDR-T1-020904-22	Provide technical performance measurement data and analysis. This reduces risk by providing preliminary data showing whether the system will meet performance requirements.	Using MIL-STD-1521B as a guide, Slides 62-65 provide data to ensure the system will meet performance requirements. Final design is still in development. Throughout the design stage, analysis will take place to ensure the system will meet performance requirements. Final presentation at CDR.	Trade Study (March '02) determined that SIGMET solution would meet all system performance requirements for processing and the receiver. Throughout the production phase, analysis and testing will take place to ensure the system will meet performance requirements. We will prepare a preliminary white paper for SW CDR.
PDR-T1-020904-27	Describe characteristics and limitations of the SIGMET signal processor and antenna controller. Early identification of limitations provides an opportunity for correction. [SIGMET Limitations]	We are conducting TIM's with RSIS and ROC to validate the signal processing performed by the SIGMET equipment. Final presentation at CDR.	SIGMET Signal Processor Discussion - Slides 51-53
PDR-T1-020904-28	Analyze alternative approaches to sending data to the RPG. Address the cost, benefits, and schedule impact for each alternative on both RDA and RPG. This would help create value to the Government for a complex design decision. At one extreme, the Government could continue with the Contract to deliver to the legacy interface (with previously agreed modifications). At the other extreme, the Government could accept a Contractor proposal to use the current SIGMET data and modify the RPG to accept it.	Slides 150-155 discuss the ORDA/ORPG Interface concerns. In addition, TIM's are taking place with SIGMET and the ROC to resolve concerns. Meeting Minutes are prepared and distributed. Final presentation at CDR.	We have completed the RDA-RPG ICD draft - Slide 86. We conducted TIMs on 9 Jan 03, and 16 Jan 03.

Action Item #	Action Item Description	RSIS Response	CDR Briefing Summary
PDR-T1-020904-54	Assembly Plan - concern that the deployment team must set up the router and system security mechanisms at each site. Potential for Access control lists passwords, etc. will not be set up correctly.	Evaluation to take place on who will set up the router and system security mechanisms. The assembly plan will document the process. This is a CDR deliverable and will be briefed at CDR.	Installation CD will automatically load configuration files for routers.
PDR-T1-020904-55	Consider alternatives, such as system-on/off test at assembly, duplicate assets to site. Objective is to reduce risk of failure at site (Slide 126)	Alternatives will be evaluated, documented in the assembly plan, and briefed at CDR.	Assembly Plan Discussion - Slides 104, 105; HW CDR Action Item 45
PDR-T1-020904-56	Is the qualification of more than one each of ORDA components a requirement (Slide 71)	We will determine if the SS and ILSP has a requirement for multiple vendors and brief it at CDR.	The SS does not require multiple vendors for components. We will qualify our component suppliers using the prototype. (Slide 75) The NRC will evaluate the availability of more than one vendor.
PDR-T1-020904-57	RCP8 & RVP8 have a unique back panel for WSR-88D. Will this have a unique part number?	The design is still in development. Evaluation is on-going to determine if a unique part number is required. The types of drawings for the ILSP is also in the evaluation process. Final presentation at CDR.	The RVP8 and RCP8 do not have unique back panels for ORDA. The I/O connector panel interfaces to both RVP8 and RCP8. Drawing Page 95
PDR-T1-020904-58	COTS components are being procured from multiple vendors. How are reliability and quality of these components assured? [Reliability]	Generic data from EMRS will be compared to the vendor specifications. Vendors are selected based upon their past history with SIGMET. Final presentation at CDR.	Maintenance Discussion - Slides 106-110
PDR-T1-020904-61	Training - please add security maintenance operator to training	Will be addressed in Training Plan. Coordination with NWSTC will take place Nov 7th, 2002. Final Presentation at CDR.	Training Plan - Slide 28; Training - Slides 117
PDR-T1-020904-62	Deployment Planning - System Site Acceptance needs to clarify who in the Gov't accepts the ORDA and assumes system is operational.	Concur - Responsibilites will be clarified and it will be briefed at CDR.	HW CDR AI 55 - COTR Designated Rep
PDR-T1-020904-63	Deployment should address special requirements of Alaska sites (Slide 147)	There are no unique requirements for the the Alaska sites. Precautions will be made by taking spare kits to the site. Information will be briefed at CDR.	Deployment Discussion - Slides 118-120. TIM 19 Feb 03
PDR-T1-020904-31	Clarify with SMEs on acceptance of Sigmet's recommended changes to operation (Slides 113 and ff.)	Concur - We are conducting TIM's with SMEs from the ROC, RSIS, and SIGMET to evaluate the SIGMET design. Meeting Minutes are prepared and distributed to CO, OST, PPD Supervision, ROC Supervision, and Agency Reps. Final Presentation at CDR.	SIGMET has agreed to design Legacy modes of operation. Our design, using Ingest, allows us to have more control to design Legacy operation. Presented at SW CDR.

Action Item #	Action Item Description	RSIS Response	CDR Briefing Summary
PDR-T1-020904-6	What is estimated impact for ORPG Development to meet security requirements (Slide 38)	The expected impact to the ORPG should not involve more than what would be expected to sustain the level of security required to operate as an accredited system, and establish a new interface to the ORDA. The ROC Security Engineering POC has already been advised of sustainment security upgrades that will be required. The ORDA security impacts will focus around the interface to the ORPG. We are intending to utilize secure tunneling methods for control commands and no longer require the X.25 protocol, thus the ORPG firewall/router function will be updated or changed. Approach to be briefed at CDR.	We will present at Software CDR.
PDR-T1-020904-9	Describe how the system security requirements are to be placed in the system baseline and tracked through testing. This would provide an understanding of the process to be used to ensure that these requirements are met.	With the National level Certification and Accreditation process, a Requirements Traceability Matrix (RTM) must be developed documenting National, Federal, and Agency level security requirements. The RTM then traces to the Information System Security Plan (ISSP) that defines the requirement in a policy or “shall” statement. These policy statements are added to the DOORS database with system security test procedures to ensure the requirement is met. System testing utilizes the DOORS requirements to validate that the system meets all requirements. Expected Completion: Approach to be briefed at CDR.	We will present at Software CDR.
PDR-T1-020904-10	Approval for the use of Java should be a high priority, as the current design efforts assume the use of Java.	A TIM was conducted with SIGMET and RSIS-Security on 5 Sept 02. It was decided that the use of JAVA will now be behind the servers for the ORDA. This will preclude any additional security authorizations. Any “unsecure” services that must be transmitted between the ORDA and ORPG will utilize secure tunneling and secured in a manner identified by agency directives. Air Force Base routers are not required of the WSR-88D system. The interface to base routers occurs with the OPUP display system. The OPUP system accreditation is currently completing the Certification and Accreditation of the System and will comply with the additional Certification of Networthiness process for data passing through the base router and direct interface into the weather office local area networks. Approach to be briefed at CDR.	We will present at Software CDR.

Action Item #	Action Item Description	RSIS Response	CDR Briefing Summary
PDR-T1-020904-12	A Vulnerability Assessment is a practical and frequently used approach to ensure that the implementation meets security requirements. Consider adding a Vulnerability Assessment to the System Security Plan.	A Vulnerability/Risk Assessment (CDRL) will be conducted separately as part of the design effort under the Management's Risk Management process. This will identify all design and operational vulnerabilities uncovered with researching the component capabilities and network/interface approach. A final Vulnerability/Risk Assessment will be completed as part of the Certification and Accreditation documentation that will provide mitigation procedures or processes to secure identified remaining vulnerabilities. Approach to be briefed at CDR.	We will present at Software CDR.
PDR-T1-020904-30	There is no software development process. How do we design to requirements? What is your design process? Where are the entrance and exit criteria for he steps in the design process? What are the entrance/exit criteria for each step in the process?	A meeting was held following PDR with RSIS Software Engineering, ROC Engineering, OST SEC, OST PPD to clarify the software development approach. The Software Development Plan will document the Software Development Process. Drafts will be sent out for review. Approach to be briefed at CDR.	We will present at Software CDR.
PDR-T1-020904-41	[System Requirements Allocation and Functional Flow] Show functional flow and requirements allocation. This would show that all requirements have been accounted and would provide insight into how the system will be able to be used.	Slide 91 represents the CI/CPCI flow. Upon completion of the analysis, requirements will be documented to the appropriate CI/CPCI. Final presentation at CDR.	We will present at Software CDR.
PDR-T1-020904-45	Some of the software will be RSIS developed; some is to be SIGMET developed. There was little discussion on the definition of the software components, who was responsible for which part, and the interfaces between these components. This points to high risk in the software integration between RSIS and SIGMET developed components.	We are conducting TIM's with SIGMET to define roles and responsibilities. Responsibility for task completion will be documented in the project plans. Final presentation at CDR.	We will present at Software CDR.